[취업폭격기 Zeromini 위클리 개념 정밀 타격 #39] [빈칸넣기문제]

📕 과목 : 정보보호론

🔥 참고문제 : 개념폭격 자료 참고 #5

[취업폭격기 Zeromini 위클리 개념폭격 #5] (정보보호론)

https://zeromini-lab.com/blog/55 내용 참고

🌝 문제 수정 버전 : V 1.0

1. 데이터의 위·변조를 방어하는 기술은 _____을 목표로 합니다.
    - 답: 무결성
    - 해설: 데이터의 무결성을 보장하는 기술은 정보가 원본 상태에서 변경, 손상, 손실 없이 유지되도록 보호하는 것을 목표로 합니다. 이는 정보보호의 핵심 원칙 중 하나로, 데이터의 정확성과 신뢰성을 유지하는 데 필수적입니다.

2. UDP 헤더 포맷에는 _____, _____, _____, 그리고 _____ 등의 구성 요소가 있습니다.
    - 답: 발신지 포트 번호, 목적지 포트 번호, 길이, 체크섬
    - 해설: UDP 헤더 포맷은 네트워크 통신에서 데이터 패킷을 전송할 때 필요한 정보를 포함합니다. 발신지와 목적지 포트 번호는 데이터가 전송되어야 할 출발지와 도착지를 나타내며, 길이는 데이터 패킷의 크기, 체크섬은 데이터의 무결성 검사를 위해 사용됩니다.
3. CSRF 공격은 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 _____하게 하는 공격입니다.
    - 답: 요청
    - 해설: CSRF(Cross-Site Request Forgery) 공격은 공격자가 사용자를 속여 사용자의 브라우저를 통해 공격자가 원하는 행위(예: 패스워드 변경, 금융 거래)를 사용자 몰래 수행하게 하는 보안 위협입니다. 이 공격은 특히 사용자가 로그인한 상태에서 발생할 때 위험하며, 웹 애플리케이션의 보안 메커니즘을 우회하여 이루어집니다.
4. IPSec의 터널 모드를 이용한 VPN은 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 _____의 IP 주소를 넣는 방식입니다.
    - 답: VPN 라우터 또는 IPSec 게이트웨이
    - 해설: IPSec의 터널 모드는 데이터 패킷 전체를 암호화하고, 그 위에 새로운 IP 헤더를 추가하여 전송하는 방식으로, 데이터의 기밀성과 무결성을 보장합니다. 이 방식은 특히 두 네트워크 간의 안전한 통신 채널을 구축할 때 사용되며, VPN 구성에 있어 핵심적인 기술입니다.
5. 대칭키 암호 알고리즘은 암호화와 복호화에 _____ 키를 사용하는 암호화 방식입니다.
    - 답: 같은
    - 해설: 대칭키 암호화 방식은 동일한 키를 사용하여 데이터를 암호화하고 복호화합니다. 이 방식의 장점은 처리 속도가 빠르다는 것이지만, 키의 배포와 관리가 주요한 도전 과제로 남습니다. 대칭키 암호화는 일반적으로 파일 암호화, 네트워크 통신 보안 등에 널리 사용됩니다.
6. 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망의 표준화 및 인증, _____의 안정성 확보 등을 규정하고 있습니다.
    - 답: 정보통신망

- 해설: 이 법률은 정보통신망을 통한 정보의 안전한 처리와 개인정보 보호, 정보통신망의 안정성과 신뢰성 확보를 목적으로 합니다. 특히, 정보통신망의 표준화 및 인증 절차를 통해 기술적, 관리적 보호 조치의 기준을 설정하고, 이를 준수하도록 규정함으로써 정보보호 수준을 높이고 있습니다.

7. 랜섬웨어는 사용자의 시스템에 침입하여 데이터를 _____하는 악성코드입니다.
   - 답: 암호화
   - 해설: 랜섬웨어는 악성 소프트웨어의 한 유형으로, 공격자가 사용자의 시스템에 침입하여 중요 데이터를 암호화합니다. 그 후, 데이터의 복호화를 위해 금전을 요구하는 형태로 피해자에게 접근합니다. 이 공격은 개인 사용자뿐만 아니라 기업이나 정부 기관에도 심각한 피해를 줄 수 있습니다.
8. SSL/TLS 프로토콜은 웹 브라우저와 서버 간의 통신을 _____하여 정보의 안전성을 보장합니다.
   - 답: 암호화
   - 해설: SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security) 프로토콜은 인터넷을 통한 데이터 전송 시 데이터를 암호화하여 보안을 강화하는 기술입니다. 이 프로토콜을 사용함으로써, 사용자와 서버 간에 전송되는 모든 데이터는 도청이나 데이터 변조로부터 보호됩니다.
9. 사이버 보안의 3가지 주요 요소는 기밀성, _____, 그리고 가용성입니다.
   - 답: 무결성
   - 해설: 사이버 보안의 핵심 원칙은 정보의 기밀성, 무결성, 그리고 가용성을 유지하는 것입니다. 기밀성은 정보가 인가된 사용자에게만 접근 가능하도록 보호하는 것을 의미하며, 무결성은 정보가 정확하고 완전한 상태를 유지하는 것, 가용성은 정보와 시스템이 필요할 때 사용 가능한 상태를 유지하는 것을 의미합니다.
10. 피싱 공격은 공격자가 가짜 웹사이트나 이메일 등을 통해 사용자로부터 _____를 빼내는 공격입니다.
    - 답: 개인 정보
    - 해설: 피싱 공격은 사회공학 기법을 사용하여 사용자를 속이고 개인 정보, 금융 정보 등을 빼내는 사이버 공격입니다. 공격자는 종종 신뢰할 수 있는 기관이나 개인을 가장하여 사용자로부터 비밀번호, 신용카드 번호 등의 민감한 정보를 획득하려고 시도합니다.
11. 웹 애플리케이션 방화벽(WAF)은 웹 애플리케이션에 대한 공격을 _____하고 차단하는 보안 솔루션입니다.
    - 답: 탐지

- 해설: 웹 애플리케이션 방화벽(WAF)은 웹 애플리케이션을 대상으로 하는 다양한 공격, 예를 들어 SQL 인젝션, 크로스 사이트 스크립팅(XSS), 크로스 사이트 요청 위조(CSRF) 등을 탐지하고 차단하는 보안 기술입니다. WAF는 웹 애플리케이션의 보안을 강화하고, 취약점을 보호하는 중요한 역할을 합니다.

12. 네트워크 침입 탐지 시스템(NIDS)은 네트워크 트래픽을 _____하며 악성 행동이나 의심스러운 패턴을 탐지하는 시스템입니다.
    - 답: 모니터링
    - 해설: 네트워크 침입 탐지 시스템(NIDS)은 네트워크를 통해 전송되는 데이터를 지속적으로 모니터링하여 알려진 공격 패턴, 비정상적인 트래픽 행동 등을 식별합니다. 이 시스템은 조직의 네트워크 보안을 강화하는 데 필수적인 도구로, 실시간으로 위협을 탐지하고 경고를 발생시킵니다.
13. 블록체인 기술은 거래 정보를 _____에 담아 체인 형태로 연결하는 분산형 데이터베이스 기술입니다.
    - 답: 블록
    - 해설: 블록체인은 거래나 기타 데이터를 '블록'이라는 단위에 저장하고, 각 블록을 암호학적으로 연결하여 체인을 형성합니다. 이 구조는 데이터의 변경이나 조작을 매우 어렵게 만들어, 높은 수준의 데이터 무결성과 보안을 제공합니다.
14. 클라우드 컴퓨팅의 서비스 모델 중 하나인 IaaS는 _____ as a Service의 약자입니다.
    - 답: Infrastructure
    - 해설: IaaS(Infrastructure as a Service)는 컴퓨팅 인프라(서버, 스토리지, 네트워크 등)를 가상화하여 인터넷을 통해 제공하는 클라우드 서비스 모델입니다. 사용자는 필요에 따라 리소스를 유연하게 할당받아 사용할 수 있으며, 사용한 만큼의 비용을 지불합니다.
15. 웹 쿠키는 웹사이트가 사용자의 브라우저에 저장하는 작은 _____ 파일로, 사용자의 세션 관리, 개인화 설정, 행동 추적 등의 기능을 수행합니다.
    - 답: 텍스트
    - 해설: 웹 쿠키는 사용자의 웹 브라우저에 저장되는 작은 텍스트 파일로, 사용자가 웹사이트를 방문할 때마다 웹사이트가 사용자를 식별하고, 사용자의 선호도나 로그인 정보 등을 기억하는 데 사용됩니다. 쿠키는 웹 사용자 경험을 개선하는 데 유용하지만, 개인 정보 보호와 관련하여 주의가 필요합니다.
16. 사이버 보안의 3가지 주요 요소인 기밀성, 무결성, 그리고 _____는 정보 시스템의 보호를 위해 필수적인 원칙입니다.

- 답: 가용성
- 해설: 사이버 보안의 핵심 원칙인 기밀성, 무결성, 가용성은 정보와 시스템이 안전하게 보호되어야 함을 의미합니다. 기밀성은 민감한 정보가 인가된 사용자에게만 접근 가능해야 함을, 무결성은 정보가 정확하고 변경되지 않아야 함을, 가용성은 정보와 시스템이 필요할 때 언제든지 접근 가능해야 함을 강조합니다.

17. SSL/TLS 프로토콜은 인터넷 통신의 보안을 강화하기 위해 데이터를 _____하여 전송합니다.
    - 답: 암호화
    - 해설: SSL(Secure Sockets Layer)과 TLS(Transport Layer Security) 프로토콜은 인터넷을 통한 데이터 전송 시 데이터를 암호화하여 보안을 강화합니다. 이러한 프로토콜을 사용함으로써, 데이터는 도청이나 변조로부터 보호되며, 통신 양 당사자의 신원도 검증할 수 있습니다.
18. 랜섬웨어 공격은 피해자의 데이터를 _____한 후, 복호화 키를 제공하기 위한 몸값을 요구합니다.
    - 답: 암호화
    - 해설: 랜섬웨어는 악성 소프트웨어의 한 유형으로, 공격자가 피해자의 데이터를 암호화하여 접근할 수 없게 만든 후, 해당 데이터를 복호화할 수 있는 키를 제공하기 위해 금전을 요구합니다. 이러한 공격은 개인 사용자뿐만 아니라 기업이나 기관에도 큰 피해를 줄 수 있습니다.
19. 정보보호의 핵심 원칙 중 하나인 무결성은 데이터가 정확하고 _____ 상태를 유지하는 것을 의미합니다.
    - 답: 변경되지 않은
    - 해설: 무결성은 정보보호의 중요한 원칙 중 하나로, 데이터가 외부의 불법적인 변경, 삭제, 조작 없이 원본의 상태를 유지하며 정확성과 완전성을 보장하는 것을 의미합니다. 무결성을 유지하는 것은 정보의 신뢰성을 보장하는 데 필수적입니다.
20. 네트워크 보안에서 IDS(Intrusion Detection System)는 네트워크 상의 비정상적인 트래픽이나 공격 시도를 _____하기 위해 사용됩니다.
    - 답: 탐지
    - 해설: 침입 탐지 시스템(IDS)은 네트워크 상의 트래픽을 모니터링하고 분석하여 비정상적인 패턴, 알려진 공격 시그니처, 의심스러운 활동 등을 탐지하는 보안 기술입니다. IDS는 조직의 네트워크 보안을 강화하고, 잠재적인 보안 위협을 조기에 식별하는 데 중요한 역할을 합니다.

21. 사이버 공격에서 흔히 사용되는 피싱(Phishing)은 사용자를 속여 _____ 정보를 획득하려는 시도입니다.
    - 답: 개인
    - 해설: 피싱은 공격자가 신뢰할 수 있는 개인이나 기관으로 가장하여 이메일, 웹사이트, 메시지 등을 통해 사용자를 속이고, 사용자로부터 개인정보, 금융정보, 로그인 자격증명 등을 획득하려는 사이버 공격 방법입니다. 피싱은 사용자의 신뢰를 악용하는 대표적인 사회공학적 공격 기법 중 하나입니다.
22. 클라우드 컴퓨팅 환경에서, 사용자가 자신의 애플리케이션을 개발하고 실행할 수 있도록 플랫폼을 제공하는 서비스 모델을 _____라고 합니다.
    - 답: PaaS(Platform as a Service)
    - 해설: PaaS(Platform as a Service)는 클라우드 컴퓨팅의 서비스 모델 중 하나로, 사용자가 인터넷을 통해 액세스할 수 있는 개발 플랫폼을 제공합니다. 이를 통해 사용자는 인프라 관리에 신경 쓰지 않고 애플리케이션 개발, 실행, 관리를 할 수 있습니다.
23. 정보보호에서, 데이터나 시스템에 접근할 수 있는 권한을 인가된 사용자에게만 부여하는 보안 원칙을 _____라고 합니다.
    - 답: 기밀성
    - 해설: 기밀성은 정보보호의 핵심 원칙 중 하나로, 민감한 정보나 시스템에 대한 접근을 인가된 사용자, 시스템, 프로세스에만 제한하는 것을 의미합니다. 기밀성 보장은 무단 접근으로부터 정보를 보호하여 정보의 비밀을 유지하는 데 중요합니다.
24. 사이버 보안에서, 악성 소프트웨어의 한 유형으로 사용자의 동의 없이 광고를 표시하거나 브라우저 설정을 변경하는 소프트웨어를 _____라고 합니다.
    - 답: 애드웨어(Adware)
    - 해설: 애드웨어(Adware)는 사용자의 컴퓨터에 광고를 표시하거나, 검색 결과를 조작하고, 브라우저의 홈페이지를 변경하는 등의 행위를 하는 악성 소프트웨어입니다. 이는 사용자 경험을 저해하고 개인 정보를 수집할 수 있는 위험을 내포하고 있습니다.
25. 정보보호 분야에서, 전자적으로 서명된 문서의 진위와 무결성을 검증하기 위해 사용되는 공개키와 개인키 기반의 기술을 _____라고 합니다.
    - 답: 디지털 서명
    - 해설: 디지털 서명은 문서나 메시지의 발신자가 자신임을 증명하고, 해당 문서나 메시지가 전송 중에 변경되지 않았음을 보증하는 기술입니다. 발신자는 개인키로 문

서를 서명하고, 수신자는 발신자의 공개키를 사용하여 서명의 진위와 문서의 무결성을 검증할 수 있습니다.

26. 네트워크 보안 기술 중 하나로, 인터넷과 같이 공개된 네트워크 상에서도 안전하게 통신할 수 있도록 가상의 사설 네트워크를 구축하는 기술을 _____라고 합니다.
    - 답: VPN(Virtual Private Network)
    - 해설: VPN(Virtual Private Network)은 공용 인터넷 인프라를 사용하여 사설 네트워크를 확장하는 기술입니다. VPN을 통해 사용자는 데이터를 암호화하여 안전하게 전송할 수 있으며, 원격 위치에서도 사내 네트워크 리소스에 접근할 수 있습니다.
27. 정보보호에서 사용되는 암호화 방식 중 하나로, 암호화와 복호화에 서로 다른 키를 사용하는 방식을 _____ 암호화라고 합니다.
    - 답: 비대칭
    - 해설: 비대칭 암호화는 두 개의 키, 즉 공개키와 개인키를 사용하는 암호화 방식입니다. 공개키는 데이터를 암호화하는 데 사용되며, 누구에게나 공개될 수 있습니다. 반면, 개인키는 암호화된 데이터를 복호화하는 데 사용되며, 키의 소유자만이 알고 있어야 합니다. 이 방식은 데이터의 안전한 전송과 디지털 서명에 널리 사용됩니다.
28. 사이버 공격 기법 중 하나로, 공격자가 시스템의 취약점을 이용하여 사용자의 세션을 가로채는 공격을 _____ 공격이라고 합니다.
    - 답: 세션 하이재킹(Session Hijacking)
    - 해설: 세션 하이재킹은 공격자가 사용자의 유효한 세션 토큰을 가로채어 사용자로 가장하여 시스템에 접근하는 기법입니다. 이를 통해 공격자는 사용자의 권한으로 데이터를 조회하거나 조작할 수 있으며, 이는 중요한 보안 위협 중 하나입니다.
29. 정보보호 분야에서, 시스템이나 네트워크에 대한 무단 접근을 방지하기 위해 사용되는 보안 장치를 _____라고 합니다.
    - 답: 방화벽(Firewall)
    - 해설: 방화벽은 네트워크나 시스템에 대한 무단 접근을 차단하고, 허용된 트래픽만을 통과시키는 보안 장치입니다. 방화벽은 물리적 장비 형태 또는 소프트웨어 형태로 구현될 수 있으며, 내부 네트워크를 외부의 위협으로부터 보호하는 중요한 역할을 합니다.
30. 웹 애플리케이션의 보안 취약점 중 하나로, 공격자가 악의적인 스크립트를 웹 페이지에 삽입하여 사용자의 브라우저에서 실행되게 하는 공격을 _____ 공격이라고 합니다.
    - 답: 크로스 사이트 스크립팅(XSS)

- 해설: 크로스 사이트 스크립팅(XSS) 공격은 공격자가 웹 애플리케이션의 취약점을 이용하여 악의적인 스크립트를 웹 페이지에 삽입하고, 이 스크립트가 다른 사용자의 브라우저에서 실행되도록 만드는 보안 위협입니다. 이 공격을 통해 공격자는 사용자의 세션 정보를 탈취하거나, 사용자를 가장하여 악의적인 행동을 할 수 있습니다.

31. 정보보호에서, 시스템이나 데이터에 대한 무단 변경을 방지하기 위해 사용되는, 데이터의 무결성을 검증하는 알고리즘을 _____라고 합니다.
    - 답: 해시 함수(Hash Function)
    - 해설: 해시 함수는 임의 길이의 데이터를 입력받아 고정된 길이의 해시값을 출력하는 함수로, 데이터의 무결성을 검증하는 데 사용됩니다. 해시 함수의 출력값은 입력 데이터에 대해 유일하며, 입력 데이터가 조금이라도 변경되면 출력값도 크게 달라집니다. 이 특성을 이용하여 데이터의 무단 변경 여부를 검증할 수 있습니다.
32. 정보보호에서, 사용자가 서비스나 시스템에 접근할 권한이 있는지를 확인하는 과정을 _____라고 합니다.
    - 답: 인증(Authentication)
    - 해설: 인증은 사용자나 시스템의 신원을 확인하는 과정입니다. 이 과정을 통해, 사용자가 주장하는 신원이 실제와 일치하는지 검증합니다. 인증 방법에는 비밀번호, 디지털 인증서, 생체 인식 등이 있으며, 이는 정보 시스템에 대한 접근 제어와 보안을 강화하는 데 중요한 역할을 합니다.
33. 정보보호 분야에서, 공격자가 정상적인 사용자로 가장하여 시스템에 접근을 시도하는 공격을 _____ 공격이라고 합니다.
    - 답: 스푸핑(Spoofing)
    - 해설: 스푸핑 공격은 공격자가 다른 사람이나 장치의 신원을 가장하여 네트워크, 웹사이트, 기타 시스템에 무단으로 접근하려는 시도입니다. IP 스푸핑, 이메일 스푸핑, ARP 스푸핑 등 다양한 형태가 있으며, 이를 통해 공격자는 민감한 정보를 탈취하거나 시스템을 손상시킬 수 있습니다.
34. 네트워크 보안에서, 데이터 패킷이 목적지까지 가는 경로를 동적으로 변경하여 공격자로부터 정보를 보호하는 기술을 _____라고 합니다.
    - 답: 패킷 레벨 암호화(Packet-Level Encryption)
    - 해설: 패킷 레벨 암호화는 데이터 패킷을 암호화하여 네트워크를 통해 전송하는 기술입니다. 이 방법은 데이터의 기밀성을 보장하고, 중간자 공격에 대한 보호를 제공합니다. 패킷의 내용뿐만 아니라 패킷의 헤더 정보까지 암호화할 수 있어, 데이터의 전송 경로도 보호할 수 있습니다.

35. 사이버 보안에서, 시스템이나 네트워크의 취약점을 주기적으로 검사하고 평가하는 활동을 _____라고 합니다.
    - 답: 취약점 평가(Vulnerability Assessment)
    - 해설: 취약점 평가는 시스템이나 네트워크에 존재할 수 있는 보안 취약점을 식별, 분류하고 평가하는 과정입니다. 이 활동을 통해 조직은 잠재적인 보안 위협을 사전에 파악하고, 적절한 보안 조치를 취하여 시스템의 보안 수준을 향상시킬 수 있습니다.
36. 정보보호에서, 데이터나 통신의 기밀성을 보장하기 위해 사용되는, 데이터를 암호화하고 복호화하는 과학적 방법을 _____라고 합니다.
    - 답: 암호학(Cryptography)
    - 해설: 암호학은 데이터나 통신의 기밀성, 무결성, 인증성을 보장하기 위해 정보를 암호화하고 복호화하는 기술과 이론을 다룹니다. 암호학은 비대칭 암호화, 대칭 암호화, 해시 함수 등 다양한 암호화 기법을 포함하며, 정보보호 분야에서 핵심적인 역할을 합니다.
37. 정보보호에서, 사용자의 신원을 확인한 후 그 사용자가 접근하려는 자원에 대한 접근 권한을 결정하는 과정을 _____라고 합니다.
    - 답: 접근 제어(Access Control)
    - 해설: 접근 제어는 인증된 사용자가 시스템이나 네트워크 내의 자원에 접근할 수 있는 권한을 관리하는 보안 과정입니다. 이 과정은 사용자가 필요한 정보에만 접근할 수 있도록 하여 정보의 기밀성과 무결성을 유지하는 데 중요합니다.
38. 사이버 보안에서, 공격자가 시스템의 취약점을 이용해 내부 네트워크에 무단으로 침입한 후, 다른 시스템으로 접근 권한을 확장해 나가는 공격을 _____ 공격이라고 합니다.
    - 답: 수직 상승(Vertical Escalation)
    - 해설: 수직 상승 또는 권한 상승 공격은 공격자가 시스템의 취약점을 이용하여 처음 침입한 낮은 권한에서 더 높은 권한의 접근 권한을 획득하는 공격 방법입니다. 이를 통해 공격자는 더 많은 정보에 접근하거나 시스템을 제어할 수 있게 됩니다.
39. 정보보호 분야에서, 전송 중인 데이터를 보호하기 위해 데이터를 보내는 측에서 암호화하고, 받는 측에서 복호화하는 프로세스를 _____라고 합니다.
    - 답: 엔드 투 엔드 암호화(End-to-End Encryption)
    - 해설: 엔드 투 엔드 암호화는 데이터를 전송하는 측에서 암호화하여, 중간에 어떤 중개자도 해당 데이터를 볼 수 없게 하고, 오직 최종 수신자만이 데이터를 복호화하여 원본 내용을 볼 수 있도록 하는 보안 프로세스입니다. 이 방식은 통신의 기밀성을 보장하는 데 매우 효과적입니다.

10. 네트워크 보안에서, 공격자가 대량의 데이터 패킷을 목표 시스템에 보내어 정상적인 서비스를 마비시키는 공격을 _____ 공격이라고 합니다.
    - 답: DDoS(Distributed Denial of Service)
    - 해설: DDoS 공격은 다수의 시스템을 이용하여 대상의 네트워크나 서버에 과도한 트래픽을 발생시켜 정상적인 서비스 제공을 방해하는 공격입니다. 이 공격은 시스템의 가용성을 저해하며, 때로는 큰 경제적 손실을 유발할 수 있습니다.